日 本 国 特 許 庁
PATENT OFFICE
JAPANESE GOVERNMENT

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日
Date of Application: １９９９年 １月１８日

出 願 番 号
Application Number: 平成１１年特許願第００９５６８号

出 願 人
Applicant (s): 日本電気株式会社

CERTIFIED COPY OF
PRIORITY DOCUMENT

１９９９年１０月 １日

特 許 庁 長 官
Commissioner,
Patent Office 近 藤 隆 彦

出証番号 出証特平１１－３０６６７７６

【書類名】　特許願

【整理番号】　66000012

【提出日】　平成11年 1月18日

【あて先】　特許庁長官殿

【国際特許分類】　G06F 12/14

【発明の名称】　機密保護機能付データ保持装置

【請求項の数】　3

【発明者】

【住所又は居所】　東京都港区芝五丁目７番１号　日本電気株式会社内

【氏名】　小久保　健一

【特許出願人】

【識別番号】　000004237

【氏名又は名称】　日本電気株式会社

【代理人】

【識別番号】　100064621

【弁理士】

【氏名又は名称】　山川　政樹

【電話番号】　03-3580-0961

【手数料の表示】

【予納台帳番号】　006194

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　9718363

【プルーフの要否】　要

【書類名】　　明細書

【発明の名称】　機密保護機能付データ保持装置

【特許請求の範囲】

【請求項１】　重要データを保持するメモリと、

筐体に設けられた複数の電極と、

筐体に対する外部からの物理的な攻撃を前記筐体に設けられた電極間の静電容量変化によって検出する重要データ管理プロセッサとを有することを特徴とする機密保護機能付データ保持装置。

【請求項２】　請求項１記載の機密保護機能付データ保持装置において、

前記重要データ管理プロセッサは、外部からの物理的な攻撃を検知したとき、前記メモリに保持された重要データを消去することにより重要データを保護することを特徴とする機密保護機能付データ保持装置。

【請求項３】　請求項２記載の機密保護機能付データ保持装置において、

筐体内の温度を検出する温度センサを有し、

前記重要データ管理プロセッサは、温度センサで検出された温度データに基づいて、温度変化に応じた筐体の形状変化による静電容量変化を補正することを特徴とする機密保護機能付データ保持装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、重要データを保持するメモリを備えたデータ保持装置に係り、特に重要データを第三者から保護する機能を備えた機密保護機能付データ保持装置に関するものである。

【０００２】

【従来の技術】

従来より、金銭データ等のデータを扱う装置の鍵となる重要データ（金銭データの書き換え及び秘匿を行うための暗号化キー等）を内部に保持している暗号化装置や課金主計装置等のデータ保持装置がある。このような装置では、金銭データの改ざんを防止するため、その鍵となる重要データが第三者によって読み出さ

れることを阻止する必要がある。

そこで、従来のデータ保持装置では、筐体の蓋にマイクロスイッチを設け、このマイクロスイッチによって筐体の開梱を検出するようにしていた。

【０００３】

【発明が解決しようとする課題】

しかしながら、以上のような従来のデータ保持装置では、マイクロスイッチの取付位置が解析されてしまうと、筐体の不正な開梱を検出できなくなり、重要データを保護できないという問題点があった。その理由は、重要データの不正な取得を目的とする第三者がマイクロスイッチの取付位置を解析すると、この第三者が、取付位置以外の部分から筐体を開ける等の対策を講じるからである。

本発明は、上記課題を解決するためになされたもので、筐体のあらゆる部分に対する物理的攻撃を検出することにより、セキュリティ機能の向上を図ることができる機密保護機能付データ保持装置を提供することを目的とする。

【０００４】

【課題を解決するための手段】

本発明の機密保護機能付データ保持装置は、重要データ（Ｄａ）を保持するメモリ（１）を有している。また、筐体（５）に設けられた複数の電極（６ａ，６ｂ，６ｃ，７ａ，７ｂ，７ｃ）と、筐体に対する外部からの物理的な攻撃を筐体に設けられた電極間の静電容量変化によって検出する重要データ管理プロセッサ（２）とを有している。

重要データを不正に取得しようとする第三者は、筐体の蓋を開けたり、筐体を壊したり、筐体に穴をあけたりする。このような筐体に対する物理的な攻撃により、筐体には力が加わり、筐体が変形する。これにより、筐体に設けられた電極間の位置関係が変化し、電極間の静電容量が変化する。重要データ管理プロセッサは、静電容量の変化を検出して、筐体に対する外部からの物理的な攻撃を検出する。

【０００５】

また、重要データ管理プロセッサは、外部からの物理的な攻撃を検知したとき、メモリに保持された重要データを消去することにより重要データを保護する。

また、前述した機密保護機能付データ保持装置の一構成例は、筐体内の温度を検出する温度センサ（４）を有している。そして、重要データ管理プロセッサは、温度センサで検出された温度データに基づいて、温度変化に応じた筐体の形状変化による静電容量変化を補正する。

【０００６】

【発明の実施の形態】

次に、本発明の実施の形態について図面を参照して詳細に説明する。図１は本発明の実施の形態を示す機密保護機能付データ保持装置のブロック図である。

本実施の形態の機密保護機能付データ保持装置は、重要データＤａを保持している重要データ保持メモリ１と、重要データ保持メモリ１を管理すると共に、外部からの物理的な攻撃を検知したとき重要データ保持メモリ１に保持された重要データＤａを消去する重要データ管理プロセッサ２と、データ保持装置としての処理を行うメインプロセッサ３と、筐体内の温度を検出する温度センサ４と、筐体５と、外部からの物理的な攻撃を検知するために筐体５に設けられた電極６ａ，６ｂ，６ｃ，７ａ，７ｂ，７ｃとから構成されている。

【０００７】

重要データＤａは、重要データ保持メモリ１に保持されている。 重要データ保持メモリ１は、重要データ管理プロセッサ２により管理されている。

データ保持装置としての実際の処理（例えば、本実施の形態のデータ保持装置が暗号化装置であれば、暗号化処理及び復号化処理）は、メインプロセッサ３によって行われる。メインプロセッサ３は、重要データ保持メモリ１に記憶された重要データＤａを処理過程において参照する必要がある場合、重要データ管理プロセッサ２を介して重要データＤａを参照する。図１において、ＣＴＬはメインプロセッサ３から出力される制御信号である。

【０００８】

図２は、筐体５への電極６ａ，６ｂ，６ｃ，７ａ，７ｂ，７ｃの設置方法を示す、図１の機密保護機能付データ保持装置の外観図である。

筐体５に設けられた電極は、電極６ａと７ａ、電極６ｂと７ｂ、電極６ｃと７ｃの３組からなり、各組を構成する対となっている２つの電極は、図２に示すよ

うに、筐体５の隣接する２つの面に設置されている。このように、電極対を３組設けているのは、筐体５の６つの面の全てに対応するためである。

【０００９】

次に、このようなデータ保持装置の動作を説明する。

重要データＤａを不正に取得しようとする第三者は、筐体５の蓋を開けたり、筐体５を壊したり、筐体５に穴をあけたりする。このような筐体５に対する物理的な攻撃により、筐体５には力が加わり、筐体５が変形する。筐体５の隣接する面に設置された対となる電極６ａと７ａの位置関係、電極６ｂと７ｂの位置関係あるいは電極６ｃと７ｃの位置関係は、筐体５の変形によって変化する。

【００１０】

電極間の位置関係が変化したことにより、電極６ａと７ａ間、電極６ｂと７ｂ間あるいは電極６ｃと７ｃ間の静電容量が変化する。この静電容量の変化は、重要データ管理プロセッサ２によって検出される。

重要データ管理プロセッサ２は、静電容量の変化を検出すると、筐体５に対して外部から物理的な攻撃が加えられたと判断し、重要データ保持メモリ１に保持された重要データＤａを消去する。

【００１１】

以上のように、本実施の形態では、筐体５に物理的な攻撃が加えられると、重要データＤａが消去される。 これにより、重要データＤａの第三者による不正な読み取りが不可能となり、重要データＤａの機密が保持される。

ところで、実際には、筐体５内部の温度変化により、筐体５の形状は熱膨張によって変化する。このような筐体５の形状変化は、上記物理的攻撃の検出に影響を及ぼす。そこで、温度変化の影響を回避する対策を以下に示す。

【００１２】

本実施の形態では、筐体５内に温度センサ４を設けている。温度センサ４は、検出した温度を温度データＤｔとして重要データ管理プロセッサ２に伝える。

重要データ管理プロセッサ２は、この温度データＤｔに基づき、温度変化に伴う筐体５の形状変化による静電容量変化を温度変化の影響が除去されるように補正する。こうして、本実施の形態では、筐体５内の温度変化による影響を受ける

ことなく、筐体５に対する物理的攻撃を正しく検出することができる。

なお、本実施の形態では、データ保持装置の例として暗号化装置を例にとって説明したが、これに限るものではないことは言うまでもない。

【００１３】

【発明の効果】

本発明によれば、筐体に対する外部からの物理的な攻撃を筐体に設けられた電極間の静電容量変化によって検出するので、従来のマイクロスイッチ方式では検出できなかった、筐体のあらゆる部分に対する物理的攻撃を検出することができ、セキュリティ機能の向上を図ることができる。

【００１４】

また、外部からの物理的な攻撃を検知したとき、メモリに保持された重要データを消去するので、重要データの不正な取得を確実に防止することができる。

【００１５】

また、温度センサで検出された温度データに基づいて、温度変化に応じた筐体の形状変化による静電容量変化を補正するので、物理的攻撃の検出に関わる温度変化の影響を回避することができる。

【図面の簡単な説明】

【図１】　本発明の実施の形態を示す機密保護機能付データ保持装置のブロック図である。

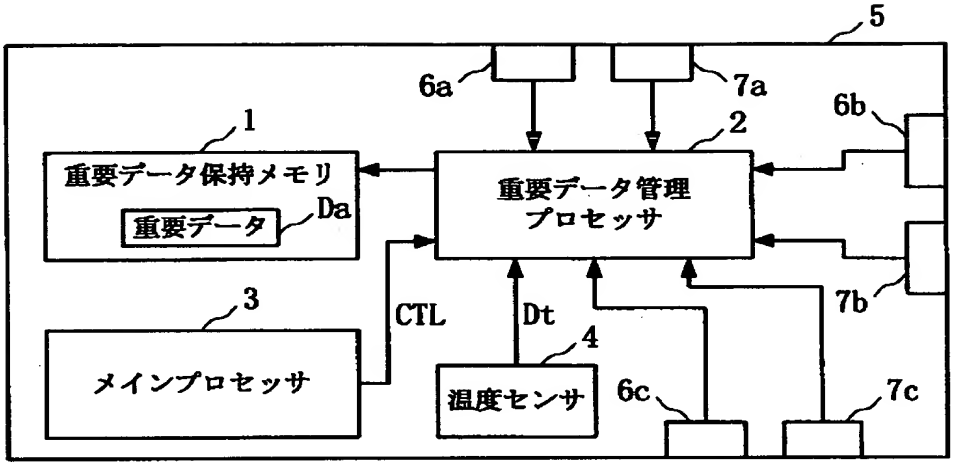
【図２】　図１の機密保護機能付データ保持装置の外観図である。

【符号の説明】

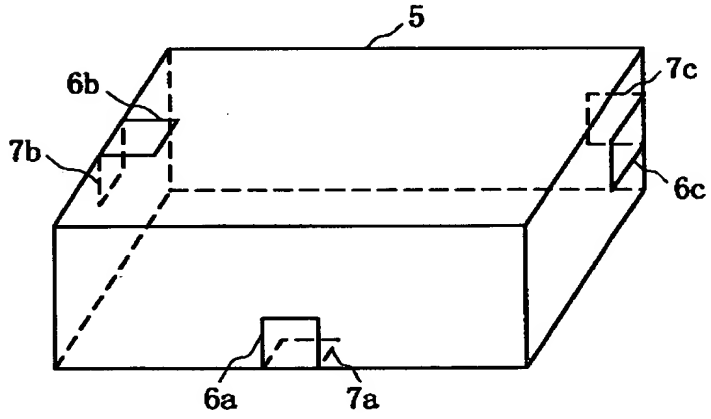
１…重要データ保持メモリ、２…重要データ管理プロセッサ、３…メインプロセッサ、４…温度センサ、５…筐体、６ａ、６ｂ、６ｃ、７ａ、７ｂ、７ｃ…電極、Ｄａ…重要データ、Ｄｔ…温度データ、ＣＴＬ…制御信号。

【書類名】　　図面

【図１】



【図２】



出証特平１１－３０６６７７６

【書類名】　　要約書

【要約】

【課題】　セキュリティ機能の向上を図る。

【解決手段】　重要データ保持メモリ１は重要データＤａを保持している。重要データＤａを不正に取得しようとする第三者は、筐体５の蓋を開けたり、筐体５を壊したり、筐体５に穴をあけたりする。筐体５に対する物理的な攻撃により、筐体５が変形する。電極６ａと７ａ、電極６ｂと７ｂあるいは電極６ｃと７ｃの位置関係は、筐体５の変形によって変化する。 電極間の位置関係が変化したことにより、電極間の静電容量が変化する。重要データ管理プロセッサ２は、静電容量の変化を検出すると、重要データＤａを消去する。

【選択図】　　図１

出　願　人　履　歴　情　報

識別番号　　〔０００００４２３７〕

１．変更年月日　　１９９０年　８月２９日
［変更理由］　新規登録
住　所　　東京都港区芝五丁目７番１号
氏　名　　日本電気株式会社